UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/760,792	01/17/2001	Jurgen Hofkens	Q62158	4947

7590 01/18/2005

SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213

EXAMINER	
GARG, YOGESH C	

ART UNIT	PAPER NUMBER
3625	

DATE MAILED: 01/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/760,792	HOFKENS, JURGEN	
	Examiner	Art Unit	
	Yogesh C Garg	3625	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 November 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,9 and 10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,9 and 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/18/2004 has been entered.

Response to Amendment

2. The applicant's amendment received on 11/18/2004 is acknowledged and entered. The applicant has amended claims 1,4,9-10. Currently claims 1,4,9 and 19 are pending for examination.

Response to Arguments

3. Applicant's arguments (see Remarks, pages 5-6) filed on 11/18/2004 with regards to amended claims have been fully considered but they are not persuasive because the newly added limitations to claims 1, 4, 9-10 are disclosed by the earlier

cited references Nguyen/Stefik. Nguyen discloses the newly added limitations "a first protector ", " a second protector" (see at least Figs. 4A-C and col.10, lines 6-67 which disclose different packets such as, security level 1, security level 2 and security level 3 are used to protect the information being transported from a sending terminal to receiver terminal. These packets of different security levels or firewalls correspond to first, second and third protectors and they are coupled as firewalls in between the sender and receiver terminals (see at least col.2, line 63-col.3, line 12, " *A network can take a variety of forms. For example, it can be two personal computers communicating via modem; it can be a single LAN system within a particular facility; it can be a remote server or mainframe system with communications links to individual terminals or personal computers; it can be a network of LANs or other servers each communicating with one another or through one another;* ***or it can be any of the foregoing systems which use not only dedicated communications lines, but also non-dedicated communications (i.e. public networks such as the Internet) through a "firewall". The use of the term firewall herein refers to the requirement for increased levels of security to avoid the possibility of unauthorized data access by parties outside of the organization.*** *Likewise, a machine in the network can act as a client or a server depending on the nature of the data transfer.* ").

Since all claims 1, 4, 9 and 10 are drawn to the same invention claimed in the earlier application and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the earlier application, this **ACTION IS MADE FINAL** even though it is a first action in this case. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 4, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nguyen in view of Stefik et al..

Regarding claim 1, Nguyen discloses a telecommunication system, for transporting information from a sender using a sending terminal to a receiver using a receiving terminal and comprising a protection mechanism for protecting said information against becoming available to at least one third party, characterized in that said protection mechanism has at least a first protector, having a first mode for protecting said information according to a first protective way, and has at least a second protector having second mode for protecting said information according to a second protective way, with said first and second protective ways being mutually different, whereby said telecommunication system is provided with an activation mechanism , coupled to said first and second protectors, for activating at least one of said first and second modes in dependence on at least control information originating from said sender and representing a value of the transported information, and in that

said protection mechanism is coupled between said sending terminal and said receiving terminal (see col.1, lines 15-20, col.1, line 65-col.2, line 12, col.2, line 60-col.3, line 12, col.7, line 39-41, col.10, lines 7-67, which disclose different packets such as, security level 1, security level 2 and security level 3 are used to protect the information being transported from a sending terminal to receiver terminal. These packets of different security levels or firewalls correspond to first, second and third protectors and they are coupled as firewalls in between the sender and receiver terminals, see at least col.2, line 63-col.3, line 12, " *A network can take a variety of forms. For example, it can be two personal computers communicating via modem; it can be a single LAN system within a particular facility; it can be a remote server or mainframe system with communications links to individual terminals or personal computers; it can be a network of LANs or other servers each communicating with one another or through one another;* ***or it can be any of the foregoing systems which use not only dedicated communications lines, but also non-dedicated communications (i.e. public networks such as the Internet) through a "firewall". The use of the term firewall herein refers to the requirement for increased levels of security to avoid the possibility of unauthorized data access by parties outside of the organization.*** *Likewise, a machine in the network can act as a client or a server depending on the nature of the data transfer.* ").

Nguyen teaches representing a value of the transported information (see at least col.3, line 65-col.4, line 55, " ..... *The random numbers Ra and the CRC signatures are then decrypted. The server calculates the CRC signature of the packet header, the user ID and the random number Ra.* ***If the calculated signatures match the decrypted signatures C1 and C2 stored in the packet, and if password Ka matches Kb, the server manipulates the client random number Ra with a predefined formula, generates a random number Rb,*** *and encrypts both random numbers Ra and Rb with the password Kb before sending the first logon response packet to the client.* .....".

Note: The generated random number Rb corresponds to the value of the transported information.).

Nguyen does not disclose that said system being further characterized in that said telecommunication system comprises a billing mechanism, coupled to said activation mechanism for billing said sender in dependence on at least the activated one of said modes. However, Stefik et al. furnishes this missing limitations (see at least Fig.1-ref.108 and col.7, lines 5-37, " ..... *Once the digital work has been transmitted to repository 2, repository 1 and 2 each* ***generate billing information for the access which is transmitted to a credit server, step 108.*** *Such double billing reporting is done to insure against attempts to circumvent the billing process.* .... ") as a required function of a system billing for the use of digital works.

In view of Stefik, it would have been obvious to one of an ordinary skill in the art at the time of the applicant's invention to have modified Nguyen (which teaches transporting data from a sender terminal to a receiver terminal via firewalls [protection mechanisms] to restrict data to authorized parties and to avoid the possibility of unauthorized data access by unauthorized parties, as already analyzed above) to incorporate the feature of a billing mechanism, coupled to said activation mechanism for billing said sender in dependence on at least the activated one of said modes because Nguyen system would be able to generate bills and send them to the users who conduct purchase transactions by ensuring security to the data being transported, such that unauthorized parties would not be able to access it.

Regarding claim 4, Nguyen further teaches that the telecommunication system according to claim 1, characterized in that said telecommunication system comprises a returning mechanism for, in response to a detection of transported information having become available to at least one third party, returning a predefined value to said sender, which predefined value is a function of said value (see col.3, line 65-col.4, line 65, "..... *The client manipulates the random number Ra with the predefined formula and compares it with the one returned from the server. If the numbers match, the client knows that it is connected to the correct server, not a fraud server from which an eavesdropper has captured transmissions from the previous logon and is echoing packets back to the client computer.* ..... .').

Regarding claims 9-10, their limitations are closely parallel to the limitations of claims 1 and 4 and they therefore are analyzed and rejected on the basis of same rationale.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

(i) US Patent 6,668,246 B1 to Yeung et al. discloses a data transportation system comprising a client-server architecture wherein a sender using a sending terminal to a receiver using a receiving terminal and comprising a protection mechanism for protecting said information against becoming available to at least one third party, characterized in that said protection mechanism has at least a first protector, having a first mode for protecting said information according to a first protective way, and has at

least a second protector having second mode for protecting said information according to a second protective way, with said first and second protective ways being mutually different, whereby said telecommunication system is provided with an activation mechanism , coupled to said first and second protectors, for activating at least one of said first and second modes in dependence on at least control information originating from said sender and representing a value of the transported information, and in that said protection mechanism is coupled between said sending terminal and said receiving terminal (see col.2, line 28-col.9, line 50).

(ii) US Patent 6,076,073 to Pieterse et al. discloses a method for protecting the data being transported related to debiting an electronic payment mechanism, such as a telephone card by using different states of a cryptographic process and to detecting an interference in the protocol (see at least abstract).

(iii) US Patent 6,687,683 to Harada et al. discloses " *A data protection system obtains data having a first content on which a first encryption has been performed and a second content on which a second encryption has been performed, the second encryption more difficult to break than the first encryption. A first content decryption unit decrypts the first content, using a first encryption method corresponding to the first encryption of the first content. A second content decryption unit decrypts the second content using a second decryption method that corresponds to the second encryption. The decrypting contents can be executed by a software, and the second content decryption unit can include one of tamperproof hardware and an apparatus that executes tamperproof software.* " (see at least abstract).

6. This is a Continuation of applicant's earlier Application No. 09/760792. All claims are drawn to the same invention claimed in the earlier application and could have been finally rejected on the grounds and art of record in the next Office action if they had been entered in the earlier application. Accordingly, **THIS ACTION IS MADE FINAL** even though it is a first action in this case. See MPEP § 706.07(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no, however, event will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh C Garg whose telephone number is 703-306-0252. The examiner can normally be reached on M-F(8:30-4:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wynn Coggins can be reached on 703-308-1344. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Yogesh C Garg
Primary Examiner
Art Unit 3625

YCG
January 12, 2005